Speaker: Luciano Maino
Title: Practical encryption from isogenies between elliptic products

Abstract. Most of the existing isogeny-based cryptographic protocols rely on computing isogenies between supersingular elliptic curves. Recent developments in isogeny-based cryptography have showed that isogenies between elliptic products in dimension > 1 can be used to break well-established cryptographic protocols. In this talk, we will explore how to employ these attack strategies to build a public-key encryption scheme. The protocol is called FESTA, which stands for Fast Encryption from Supersingular Torsion Attacks. Its practical performance is achieved leveraging fast formulae for (2,2)-isogenies.

N.B. This is joint work with Andrea Basso and Giacomo Pope.